



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350 -2000

IN REPLY REFER TO
OPNAVINST 2221.5B
OP-944

5 SEP 1984

OPNAV INSTRUCTION 2221.5B

From: Chief of Naval Operations

Subj: RELEASE OF COMMUNICATIONS SECURITY (COMSEC) MATERIAL
TO U. S. INDUSTRIAL FIRMS UNDER CONTRACT TO THE
U. S. NAVY

Ref: (a) DOD Supplement 5220.22-S-1 (COMSEC Supplement to
the Industrial Security Manual for Safeguarding
Classified Information) of August 1983 (NOTAL)
(b) DOD Manual 5220.22-M (Industrial Security Manual for
Safeguarding Classified Information) of March 1984
(NOTAL)

1. Purpose. To revise policy and expand procedures for authorizing release of COMSEC material to U. S. industrial firms under contract to the U. S. Navy.

2. Cancellation. OPNAVINST 2221.5A. (R)

3. Applicability. The following terms are defined as applicable to this instruction: (A)

a. COMSEC material - COMSEC aids (e.g., keying material, operating and maintenance manuals), equipments and components thereof, and devices which are identifiable by the Telecommunications Security (TSEC) nomenclature system or a similar system of a U. S. department or agency, foreign government, or international organization.

b. COMSEC equipment - crypto-equipment, crypto-ancillary equipment, and authentication equipment.

c. COMSEC information - all information relating to COMSEC material and COMSEC equipment.

4. Policy. Government cryptographic equipment operations will ordinarily be conducted by the Government. However, when there is a valid need and it is clearly in the best interest of the Navy and the Government, cryptographic equipment, keying material, related COMSEC information, and access to classified U. S. Government traffic may be provided to U. S. contractors to:

a. Install, maintain, or operate "TSEC" nomenclatured COMSEC equipment for the U. S. Government.

b. Participate in the design, planning, production, training, installation, maintenance, operation, logistical

5 SEP 1984

support, integration, modification, testing, or study of COMSEC material or techniques.

- R) c. Electrically communicate classified national security information in a cryptographically secure manner, or unclassified national security-related information by COMSEC protected means.
- R) 5. Requirements. Contractor personnel who are granted access to COMSEC material must be U.S. citizens. Such access shall be controlled on a strict need-to-know basis and shall be granted only in conformance with procedures established for the particular type of COMSEC information involved. Detailed guidance for contracting offices concerning security clearances, access authorization, and briefings are set forth in references (a) and (b). All contracts involving COMSEC material with industrial firms must contain the following information:
 - A) a. U.S. cryptographic equipment inventory information, as well as the systems and manner in which each particular equipment is used, is for official use only. Publication or release of any related COMSEC information by any means, by the commercial firm, without prior written approval of the contracting office is prohibited.
 - A) b. Individuals granted access to classified COMSEC material must hold a final Government security clearance for the level of classification involved. The clearances of facility security officers, COMSEC custodians, and alternate COMSEC custodians must be predicated on a favorable background investigation current within five years.
 - A) c. All individuals provided access to COMSEC material must be briefed at least annually regarding the unique nature of COMSEC material and their security responsibilities to safeguard and control it.
 - A) d. All individuals who maintain Government cryptographic equipment (TSEC) must receive formal NSA-approved training on such equipment.
- 6. Action. Prior to release of any COMSEC material to a U.S. industrial firm under contract to the U.S. Navy for one of the purposes described in paragraph 4, the contracting office shall submit a request to the Commander, Naval Security Group Command (COMNAVSECGRU) for review and approval. Provide a copy to the Chief of Naval Operations (OP-941 and OP-944), Commander, Naval Telecommunications Command, and Director, Communications Security Material System (DCMS). The request shall include sufficient justification upon which to base a decision that such

5 SEP 1984

- A) a. Identify the individual and/or organization, their citizenship, their level of security clearance, and the location(s) at which COMSEC functions will be performed.
- A) b. Identify the COMSEC functions the nongovernment source(s) will perform, the COMSEC material to which the individual(s) will have access, the number of personnel involved, their training certification or any training required.
- A) c. List the classification of the COMSEC material to which the source personnel will have access.
- A) d. Indicate whether source personnel will be using keying materials marked "CRYPTO" which are held or used by Government departments and agencies. If so, has consideration been given to providing unique operational keying materials?
- A) e. Indicate what additional administrative/security measures will be implemented.
- A) f. Identify the inclusive dates for which source personnel will have access to COMSEC material under the provision of the contract or arrangement.
- A) g. Identify the Government department or agency which will be responsible for assuring the security of nongovernment cryptographic operations/functions.
- A) h. Identify the specific provisions of this instruction for which an exception is required.

9. Continuing Action. COMNAVSECGRU shall be kept informed for the life of the contract of any events that affect the length of the contract or the type and amount of COMSEC material involved. COMNAVSECGRU shall also be notified of the date of the actual termination of the contract.


E. E. KIRKSEY
By direction

Distribution:

SNL	A1	(Immediate Office of the Secretary)
	A2A	(Department of the Navy Staff Offices) (Chief of Naval Research, only)
	A3	(Chief of Naval Operations)
	A4A	(Chief of Naval Material)

5 SEP 1984

release is in the best interest of the Navy and the Government and a statement that all applicable requirements of this instruction and references (a) and (b) have been met. Additionally, the following applicable information shall be included in the request:

a. Contract number, name of contractor, licensee, or individual; facility clearance; and location at which the functions will be performed.

b. Nature and scope of the contractual functions; the COMSEC material or cryptographic equipment to which the contractor personnel will have access; and the number of contractor personnel involved.

c. In the case of contractor operation of a secure telecommunications facility, the classification and type of material involved and whether access to U.S. Government traffic will be supervised by government civilian or military personnel.

d. The initial date on which contractor personnel will have access to COMSEC material or equipment and the length of the contract or period of time such access will be required.

e. Description of any additional administrative or security measures over and above the requirements of this instruction or of references (a) and (b), which will be implemented to ensure that contractor personnel will not gain access to classified information or material for which they do not possess a security clearance and valid need-to-know.

7. Accounts. COMSEC accounts established at contractor facilities in accordance with reference (a), as a result of Navy contracts, are NSA accounts administered by the Director, National Security Agency (DIRNSA). DCMS will assist in establishing COMSEC accounts as necessary.

8. Approval. COMNAVSECGRU shall review each request received to ensure that all the requirements of the national policy for release of COMSEC material to U.S. industrial firms are fulfilled; approve the release from a national policy aspect; and advise appropriate commands and the DIRNSA of the approval so that other required action can be initiated. In the event the provisions of this instruction cannot be met and sufficient justification for release to contractor personnel is provided, the COMNAVSECGRU will initiate action to request an exception to the national policy from the National Communications Security Committee. The following checklist should be used as a guideline in requesting exceptions to this policy:

5 SEP 1984

A6 (Headquarters, U.S. Marine Corps)
 B1A (Secretary of Defense)
 B2A (Special Agencies, Staffs, Boards, and Committees)
 (Director, Defense Communications Agency; Director
 Defense Logistics Agency; and Director, National
 Security Agency, only)
 B2D (Defense Contract Administration Service Regions)
 B3 (College and University)
 B5 (U.S. Coast Guard) (Commandant, only)
 21A (Fleet Commanders in Chief)
 22A (Fleet Commanders)
 23 (Force Commanders)
 24 (Type Commanders)
 26F (Operational Test and Evaluation Force and
 Detachment)
 41A (Commander, MSC)
 41B (Area Commanders, MSC)
 E3A (Laboratory, ONR)
 FA22 (Oceanographic System LANT)
 FB38 (Oceanographic System PAC)
 FD1 (Naval Oceanography Command)
 FF1 (Naval District, Washington, D.C.)
 FF62 (Chief of Naval Reserve)
 FG1 (Telecommunications Command Headquarters)
 FG6 (Communication Area Master Station)
 FKAlA (Air Systems Command Headquarters)
 FKAlB (Electronics Systems Command Headquarters)
 FKAlC (Facilities Engineering Command Headquarters)
 FKAlF (Supply Systems Command Headquarters)
 FKAlG (Sea Systems Command Headquarters)
 FKQ2 (Electronic Systems Security Engineering Center)
 FS1 (Intelligence Command Headquarters)
 FT1 (Chief of Naval Education and Training)
 V12 (Marine Corps Development and Education Command)

Defense Investigative Service, Washington, D.C.

Stocked

CO, NAVPUBFORMCEN

5801 Tabor Ave.

Philadelphia, PA 19120 (100)